

STATE OF OHIO



DEPARTMENT OF REHABILITATION
AND CORRECTION

SUBJECT: Surveillance	PAGE <u>1</u> OF <u>7</u>
	NUMBER: 09-INV-01
RULE/CODE REFERENCE: ORC 2933.51	SUPERSEDES: 09-INV-01 dated 05/26/14
RELATED ACA STANDARDS:	EFFECTIVE DATE: September 3, 2015
	APPROVED: 

I. AUTHORITY

This policy is issued in compliance with Ohio Revised Code 5120.01 which delegates to the Director of the Department of Rehabilitation and Correction the authority to manage and direct the total operations of the Department and to establish such rules and regulations as the Director prescribes.

II. PURPOSE

The purpose of this policy is to establish operational guidelines for the appropriate use of surveillance within or on the grounds of a correction institution or other Ohio Department of Rehabilitation and Correction (DRC) office or facility. These guidelines also apply to locations outside the jurisdiction of the DRC, as appropriate, within the scope of an authorized investigation.

III. APPLICABILITY

This policy applies to all persons employed by the Ohio Department of Rehabilitation and Correction (DRC), independent contractors providing a service to the Department, inmates, and volunteers.

IV. DEFINITIONS

Legally Recognized Privileged Communication - Any communication that is considered confidential under the law or DRC policy including communication: between an attorney-client; between physician-patient; or with a psychologist, psychiatrist, minister, priest, or clergy.

Surveillance – The observing, monitoring, gathering, recording or intercepting of activities, information, conversation or evidence through the authorized and lawful use of personnel or equipment. The surveillance of individuals or areas may be conducted by overt or covert methods of operation through use of the physical human senses and/or electronic and mechanical devices. Electronic surveillance may be achieved by utilization of radios, cameras, equipment, transmitters, tape recorders, extension telephones, telephone switchboard, video or other such equipment, means or devices.

V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction (DRC) to ensure surveillance within a correctional institution, other DRC office, or facility is conducted in a manner consistent with legal requirements. In cases where surveillance is used as part of an official investigation involving parolees, community release or other individuals or conducted at locations other than those under the jurisdiction of the DRC, these same legal requirements must be met.

VI. PROCEDURES**A. Inmate Telephone Conversations**

1. Inmate conversations conducted on telephones provided specifically for their use are not considered private and may be monitored and/or recorded. Department Policy 76-VIS-02, Inmate Access to the Telephone, provides procedures for privileged communications.
2. Inmates shall be informed, both during orientation and through the inmate handbook, that telephone calls may be monitored and that any privileged communication should be accomplished by mail or in person.
3. Signs stating that calls are subject to monitoring and recording shall be posted in the immediate vicinity of every inmate telephone.
4. Notice to inmates during orientation and the inmate handbook shall explicitly state that all inmate telephone calls are subject to being monitored and/or recorded and that any inmate who uses the telephone must consent to such monitoring as a condition of being allowed to use the telephones.
5. Inmates shall be informed, both during orientation and through the inmate handbook, that 3-way calls and call forwarding are strictly prohibited.

B. Inmate Electronic Mail (email)

1. All content contained in an Email system provided specifically for inmates is not considered private and may be monitored and/or copied in an electronic or paper format.
2. Inmates shall be informed, both during orientation and through the inmate handbook, that their Emails may be monitored and that any privileged communication should be accomplished by mail or in person.
3. Signs stating that Email is subject to monitoring or copying shall be posted in the immediate vicinity of every inmate Email computing device.
4. Notice to inmates during orientation and the inmate handbook shall explicitly state that all inmate Emails are subject to being monitored and/or copied in an electronic or paper format and that any inmate using the Email system provided specifically for them must

consent to such monitoring and/or copying as a condition of being allowed to use said Email system.

5. Inmates shall be informed, both during orientation and through the inmate handbook, that forwarding Emails to others not approved to receive them is strictly prohibited.

C. Employee Telephone Conversations

Employee or contractor telephone conversations, where either one or both parties are using DRC telephone instruments, may not be electronically monitored unless there is one-party consent or a court order.

D. Surveillance Cameras

1. DRC surveillance cameras, their associated monitoring software and the resulting video images are used in DRC correctional institutions, offices and other facilities to ensure safe, secure and humane operations that support the security and rehabilitative mission of DRC. They shall only be used by authorized DRC staff and other authorized individuals and only for approved DRC business purposes.
2. In order to maintain the required camera equipment and software technological requirements and standards, all surveillance cameras, servers, and/or associated software/hardware purchases for DRC correctional institutions, offices or facilities shall be submitted to the Chief of the Bureau of Information Technology Services (BITS) for prior approval. An Enterprise level licensure of the On-Net Surveillance Systems Inc. (OnSSI) video management system software shall be maintained by BITS.
3. Pursuant to Department Policy 79-ISA-01, Prison Rape Elimination, when surveillance cameras or the associated monitoring software are installed in DRC correctional institutions, or when the equipment or software are updated in DRC correctional institutions, the appropriate DRC administrators shall consider how the camera and software technology may enhance DRC's ability to protect inmates from sexual abuse. This consideration shall be documented in written form and forwarded to DRC's Agency PREA Coordinator and all appropriate DRC Regional Directors.
4. The following procedures shall be followed when DRC surveillance cameras or the associated monitoring software are installed:
 - a. In DRC correctional institutions, the Managing Officer or designee in consultation with the institutional Operational Compliance Manager and Chief of BITS or designee shall:
 - i. Identify the appropriate locations for the cameras.
 - ii. Ensure that the monitoring software is configured pursuant to policy.

- iii. Oversee installation of the cameras.
 - b. In DRC offices and other facilities, the appropriate Deputy Director or designee in consultation with the Chief of BITS or designee shall:
 - i. Identify the appropriate locations for the cameras.
 - ii. Ensure that the monitoring software is configured pursuant to policy.
 - iii. Oversee installation of the cameras.
 - c. The Chief of BITS shall assign the appropriate BITS staff members to assist in scheduling, coordinating and completing the installation of the surveillance cameras and associated software in DRC correctional institutions, offices or facilities.
5. Access to the DRC surveillance camera system shall be limited to the following DRC staff members:
 - a. The Chief Legal Counsel or designee.
 - b. The Chief Inspector or designee.
 - c. The Agency PREA Coordinator or designee.
 - d. The Chief of BITS or designee.
 - e. In DRC correctional institutions, the Managing Officer or designee shall approve necessary staff and their required level of access.
 - f. In DRC offices and other facilities, the appropriate Deputy Director or designee shall approve necessary staff and their required level of access.
 - g. The OSC BITS technicians and the local technicians assigned by the Chief of BITS or designee or Managing Officer or designee to maintain and support the DRC surveillance camera system and the associated software on the enterprise and local levels.
6. In order to document and track access to the DRC surveillance camera system, a video surveillance system user access log listing approved users and their level of access shall be maintained by the Managing Officer or designee in DRC correctional institutions or the appropriate Deputy Director or designee in DRC offices and other facilities. The Chief of BITS or designee shall review copies of the logs at regular intervals to audit DRC surveillance camera system user accounts.
7. The following DRC staff members shall have the authority to block another staff member's access, on a temporary or permanent basis, from viewing real time or copied/saved/stored surveillance camera video images:
 - a. The Chief Legal Counsel or designee.
 - b. The Chief Inspector or designee.
 - c. The Agency PREA Coordinator.

- d. The Chief of BITS or designee.
 - e. The Managing Officer or designee in DRC correctional institutions.
 - f. The appropriate Deputy Director or designee in DRC offices and other facilities.
8. Video images captured on DRC surveillance cameras shall be copied/saved/stored only on an approved and physically secure DRC computing device such as a server, desktop computer, portable computing device or portable computing media, and only when approved by:
- a. The Chief Legal Counsel or designee.
 - b. The Chief Inspector or designee.
 - c. The Agency PREA Coordinator.
 - d. The Chief of BITS or designee.
 - e. The Managing Officer or designee in DRC correctional institutions.
 - f. The appropriate Deputy Director or designee in DRC offices and other facilities.
9. The viewing of copied/saved/stored DRC surveillance camera video images shall be limited to the following DRC staff members:
- a. The Chief Legal Counsel or designee.
 - b. The Chief Inspector or designee.
 - c. The Agency PREA Coordinator
 - d. The Chief of BITS or designee
 - e. The Managing Officer or designee in DRC correctional institutions.
 - f. The appropriate Deputy Director or designee in DRC offices and other facilities.
10. The following retention guidelines apply to video images captured on DRC surveillance camera systems:
- a. All video images reviewed as part of an official DRC investigation or official DRC administrative process, including but not limited to, the use of force review process, the inmate disciplinary process, the PREA investigative process, the employee disciplinary process, etc. shall be subject to the following provisions. In addition, all video images specifically captured on DRC surveillance cameras to record a planned event or transition, such as a use of force or an investigation, shall be:
 - i. Noted or referenced, even if not relied upon, in the investigative or administrative record or report.
 - ii. Copied/saved/stored and then retained as part of the investigative or administrative record.
 - iii. Maintained and retained in the investigative or administrative record or file pursuant to the applicable DRC Retention Schedule, including but not limited to, Special Investigation Case Files, ADEX-001; Use of Force Reports, ADEX-0029:

Equal Opportunity Case Files/Active and Inactive Discrimination Complaint Files, HR-0011; Disciplinary Records, REC-0032; Rules Infraction Board Recordings, REC-0049; Probationary Removal, HR-0034; Personnel Board of Review File, HR-0035; Personnel Records and Confidential File, HR-0036.

- b. When video images captured on a DRC surveillance camera are part of any matter being litigated or a “litigation hold letter” is issued for video images captured on a DRC surveillance camera or an investigative or administrative record or file containing video images captured on a DRC surveillance camera, the video images shall not be destroyed and shall be maintained and retained until released by DRC Legal Services.
 - c. Video images not reviewed as part of an official DRC investigation or official DRC administrative process, not specifically captured on DRC surveillance cameras to record a planned event or transaction, or not part of any matter being litigated or being retained pursuant to a “litigation hold letter” shall be retained a minimum of 14 calendar days.
11. The location and/or viewing area of existing surveillance cameras shall not be moved/changed/alterd without the written approval of the Managing Officer.

E. Covert Surveillance

1. Any electronic surveillance beyond the routine monitoring of inmate telephones, mail and non-covert cameras shall require written notification to and approval from the respective Regional Director and the Chief Inspector prior to the implementation of electronic surveillance by DRC staff. If time is of the essence, verbal approval may be granted and documented by either the Regional Director or the Chief Inspector and, if deemed necessary by the circumstances, incidental use of cell phone cameras may be utilized for the electronic surveillance. However, written notification and approval must be sent and received by the Chief Inspector and the respective Regional Director within the next twenty-four hours after verbal authorization has been granted.
2. The request to utilize electronic surveillance shall include, but not be limited to:
 - a. The date and estimated length of time electronic surveillance will be used.
 - b. One-party consent or court order, for electronic surveillance of audio.
 - c. Type of electronic surveillance being used.
 - d. Location in the institution, or other area, where the electronic surveillance will be conducted.
 - e. Documentation of notice and/or approval of the Managing Officer.

- f. Any other information necessary in determining the necessity and risk involved in the operation.
3. Approval for installation and/or use of electronic surveillance equipment during the course of an investigation conducted by the Ohio State Highway Patrol is not required. However, when practicable and prior to implementation, notification shall be provided to the respective Regional Director and Chief Inspector. Such notification shall contain, in general, the information noted in section VI(D)(2) above.

F. Warrants

If, for the safety and security of the institution, it becomes necessary to obtain a warrant allowing monitoring or interception of communications in a manner not allowed by this policy, a request for such a warrant should be directed to the chief inspector. The Chief Inspector shall evaluate such a request, apprise the appropriate Regional Director and take further action as appropriate.